

---

# Fingerprinting All AI Cluster I/O Without Mutually Trusted Processors

---

Naci Cankaya  
MATs Fellowship

Jakub Kryś  
SaferAI

Jonathan Ng  
Independent

Luke Marks  
Martial

Felix Krückel  
RWTH Aachen University

## Abstract

In preparation for potential international agreements on artificial intelligence, the development of verification infrastructure is vital. We propose a method for fingerprinting AI cluster activity based on tapping network traffic in and out of datacenters. These fingerprints enable an auditor (the “verifier”) to retroactively challenge the original data to be sent to a privacy-preserving verification facility. Our main goal is to make it infeasible to covertly exfiltrate results of undisclosed workloads in the cluster. To this end, we propose using a retrofittable “border patrol” device configured to be the only communication channel between the datacenter and the outside world. Our contribution is the architecture and simulation of such a device, which also handles erasure of those covert channels which post-hoc verification on fingerprints cannot address: Analog and timing side-channels, as well as steganography in network protocol headers. The architecture eliminates the need for any mutually trusted processors, leveraging the physics of simple, passive optical fiber splitters and coin-flip protocols for random number generation where needed. We expect development costs of a demonstration device to be well below \$2MREMEMBER THIS NEEDS JUSTIFICATION. We make available our code at <https://github.com/derpypl0ps/warden>, as well as a visualisation of the device function at <https://www.felix-krueckel.com/warden.html>.

## 1 Introduction

The rapid progress of Artificial Intelligence (AI) in recent years has opened the door to accelerating advancements in multiple fields including medicine, engineering or computer science. However, as a very powerful general-purpose tool, AI also exacerbates existing concerns around technology misuse, as well as introduces novel risk vectors such as the threat of autonomous misaligned agents [Yoshua Bengio et al., 2026]. For this reason, several jurisdictions have already introduced legally-binding regulations governing the acceptable uses, transparency obligations or testing requirements of generative AI systems [China Law Translate, 2023, European Parliament, 2024, Wiener, 2025]. Additionally, in the future the need and political will for treaties and agreements might also arise between jurisdictions. For example, in recognition of the tremendous power afforded by AI, leading actors in this technology competition could agree on ‘red lines’ that neither of them should cross [CeSIA and The Future Society, 2025]. These may emulate historical agreements in other safety-critical areas such as The Nuclear Non-Proliferation Treaty or START.

Regardless of the nature of such legislation or treaties, there is a clear need for the ability to verify compliance with the rules by all affected parties. This problem is particularly important and challenging in the context of AI, since computing power as a resource has a much more dual-use nature than fissile materials or even DNA synthesis tools [Sastri et al., 2024]. Consequently, the field of AI Verification has recently emerged as a maturing research agenda spanning both technical and governance aspects. The importance of robust verification mechanisms is reflected by the appearance in literature of three major works detailing open problems, policy goals and possible research directions in this area [Scher and Thiergart, 2024, Harack et al., 2025, Brundage et al., 2025]. These are presented concisely in Fig. 1.

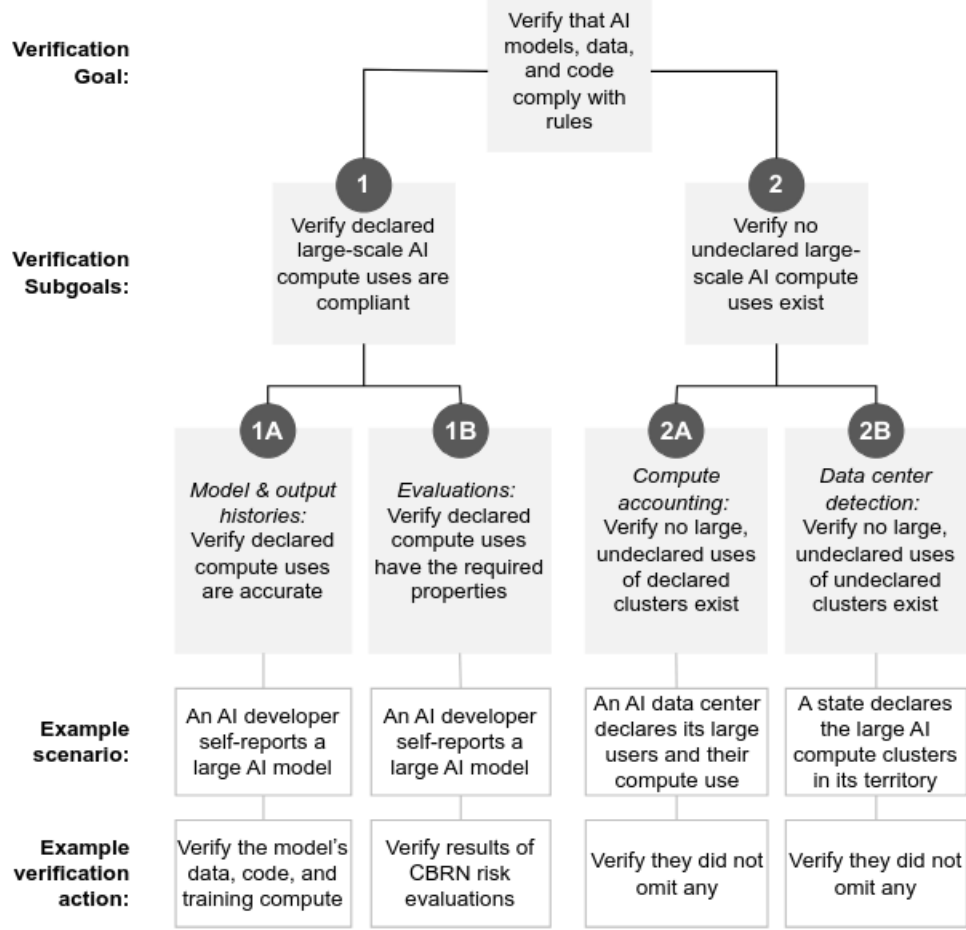


Figure 1: A breakdown of the AI Verification research agenda into its goals and subgoals. Reproduced from Brundage et al. [2025] with authors' permission. In this work, we focus on verification Subgoal 2A.

In this work, we contribute to Subgoal 2A, which can be summarised as follows. An entity operating a computing cluster — the Prover — declares to the party imposing regulations — the Verifier — that they intend to execute certain workloads on this cluster that are compliant with such rules. The Verifier wishes to ensure that the Prover is not executing other, that is undeclared, workloads on this cluster. In other words, they verify the *comprehensiveness* of the declared cluster usage. Crucially, we do not tackle the problem of determining which workloads should be allowed or not in the first place (*regulation*) or of verifying whether the declared workloads are allowed (*compliance*, Goal 1). **Our scope is exclusively to verify that the declared workloads constitute all the workloads that have been actually executed, regardless of whether they are compliant or not.** We also do not consider the threat vector of hidden compute clusters (Subgoal 2B).

Most solutions for verifying compliance and comprehensiveness proposed so far focus on mechanisms that can be fitted on or around hardware accelerators [Aarne et al., 2024]. These include devices such as Trusted Execution Environments, HBM-based chiplets that monitor traffic in and out of the memory stacks [Petrie, 2025] and tamper-proof enclosures to house the accelerators [Happel, 2026]<sup>1</sup>. Instead of targetting individual accelerators, in this paper we operate at the level of the whole data centre. In particular, we focus on the communication chokepoint between that hardware and the Prover: the datacenter north-south internet uplink. If the Verifier can capture, hash and timestamp *all*

<sup>1</sup>For a thorough overview of possible directions, we refer the reader to the three-part series by the FlexHEG initiative [FlexHEG Initiative, 2025].

traffic in and out of the datacenter, and the Prover can — upon later request — demonstrate that their declared workloads correspond to this hashed traffic, the Verifier can be satisfied that the Prover is not performing undeclared computations in the cluster. To achieve this goal, we propose a schematic design of a ‘Border Patrol’ device that uses passive network taps [INSERT REFERENCE] to capture and process such traffic for later verification in a mutually trusted manner.

### Main contributions

1. A detailed description of the problem statement and the design requirement for a verification mechanism meant to address Subgoal 2A of Brundage et al. [2025] (Section 3).
2. An actionable design specification of our proposed Border Patrol device that addresses these requirements. This includes a detailed description of how the device processes captured traffic in order to eliminate steganographic degrees of freedom in egress data (Section 4).
3. A feasibility assessment of this solution, including estimating the storage requirements needed for the associated verification protocol (Section 5).
4. A demonstration of the intended functioning of the device using simulated I/O data centre traffic (Section 6).

## 2 Related Work

We draw from research by Fisk et al. [2003] and Xing et al. [2020] on active wardens for erasing steganography channels in protocol headers, as well as Lee et al. [2014] and Uttarwar and Dakhane [2025] for erasing timing side-channels by adding jitter in a bump-in-the-wire <- what is this?. Both methods are part of our proposed Border Patrol device. While replay verification is not part of our project scope, we refer to Karvonen et al. [2025] and Cankaya [2026] for highlighting the importance of this downstream challenge for closing off exploitable degrees of freedom [Rinberg et al., 2025] in the replay’s inaccuracy if not mitigated. THIS NEEDS TO BE EXPANDED, AT LEAST WITH MORE EXPLANATION. CURRENTLY IT’S SUPER TECHNICAL. ALSO NEED TO TALK ABOUT: NETWORK TAPS, STEGANOGRAPHY, SIDE CHANNEL ATTACKS, TIMING ATTACKS, ETC.

## 3 Problem statement

We are interested in designing a device which allows the Prover to demonstrate the *comprehensiveness* of its declared workloads to the Verifier. This introduces the following requirements:

1. The device needs to capture all of the ingress/egress traffic of a data centre.
2. It must be mutually trusted by both Prover and the Verifier. This means that:
  - The Prover must not have the ability to hide significant amounts of information in the traffic being monitored. Otherwise, they could transfer undeclared workloads out of the data centre using steganographic techniques, side-channels, timing attacks, and similar.
  - The Verifier must not have the ability to extract Prover’s proprietary information out of the device.
3. The solution should be retrofittable to realistic, full-scale deployments at the scale of  $\mathcal{O}(100k)$  accelerators. To the extent possible, it should rely on existing and affordable technologies.
4. The device should introduce as little additional latency as possible in order to minimise the slowdown of usual data centre operations. It should be able to process millions of communication packets streaming in/out every second.

We are working under the following assumptions:

- We focus on traffic serving LLM API endpoints to external customers. We also assume most API traffic is egress, not ingress. This is because customer traffic served via the ‘streaming API’ format, commonly used for chatbot applications, is optimised for low latency in delivering responses to customers at the cost of high data inefficiency (see e.g., OpenAI [2025]). Every single output token is wrapped in a JSON packaging adding  $\sim 200$  bytes of overhead<sup>2</sup>.

---

<sup>2</sup>Strictly speaking, streaming responses may contain batches of a few tokens, although in practice the number is exactly one. We take this simplifying assumption because we are also interested in a worst-case feasibility

- Steganography via *input* payload data (i.e., the plaintext requests to the LLM) is unconstrained<sup>3</sup>. However, the output payload’s strict causal dependence on the **declared** inputs is verified post-hoc, based on the evidence captured by the border patrol device. Only payload data is hashed, as protocol header nonces would otherwise need to be stored long-term **I DON’T THINK THIS SHOULD BE HERE**.
- The Prover needs to store all information that forms a part of the hash for as long as is required by the Verifier. In practice, this includes both the plaintext response data and the associated JSON metadata.

### Out of scope

In order to convey the nuance of the problems we are — and are not—tackling, we briefly explain the “verification pipeline” we are assuming:

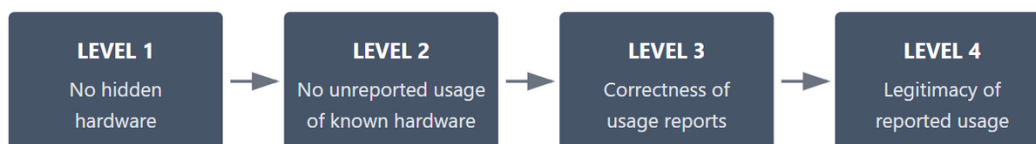


Figure 2: Your caption here

- We consider only text inputs and outputs. Audio, image and video generation are out of scope. These could potentially increase the storage requirements of our method, as well as introduce novel steganographic degrees of freedom that ought to be accounted for.

We are specifically aiming for level 2: Capturing raw evidence of computation (only hashes, not plaintext). The hashes, together with the plaintext data it points to, would later feed into a secure cluster trusted by the verifier, without the plaintext information being shown to them directly.

The verification in said cluster is twofold, and out of scope for us: replaying observed inputs and outputs to confirm they match precisely<sup>4</sup> (level 3), and evaluating the computations for legal compliance (level 4).

Also out of scope of this work is the physical monitoring of both the prover’s cluster and the verification facility needed to prevent secret communication *devices*. Finally, we do not go into detail on steganographic degrees of freedom in unverifiable information contained in application layer payloads (e.g. a limit on GPU temperature diagnostics leaving the facility). These degrees of freedom are not for our border patrol device to erase, but for rules to constrain<sup>5</sup>.

## 4 Methods

**THIS NEEDS A MUCH LONGER INTRODUCTION COVERING EACH COMPONENT, ITS FUNCTION AND WHY ITS NECESSARY** We recommend using our interactive demonstration [web, 2026h] of how our evidence capture device (“border patrol”) works. In addition, we give a more detailed treatment of our method and setting below. **The most important points about the macroarchitecture (placement of the border patrol device):**

1. The facility is under physical monitoring, ensuring that any traffic in and out of the cluster needs to pass through the border patrol chokepoint.
2. Every bit of traffic sent to the verifier (hashes only) can be passively observed by the prover. This places the root of trust in *physics*: Beam splitting via FBT or PLC [web, 2026d] (glass touching glass) and optical isolators [web, 2026e] (one-way-street) ensure the prover can

assessment of the Border Patrol solution. With only 1 token per streaming response, the amount of data produced represents an upper bound for the storage requirements of our method.

<sup>3</sup>The warden device could in principle rewrite prompts and input media files while preserving semantics. However, this carries complications related to a potential degradation of the LLM’s performance. We leave this open for future research.

<sup>4</sup>Same as previous footnote.

<sup>5</sup>Since this information is hashed, compliance checking here is trivial.

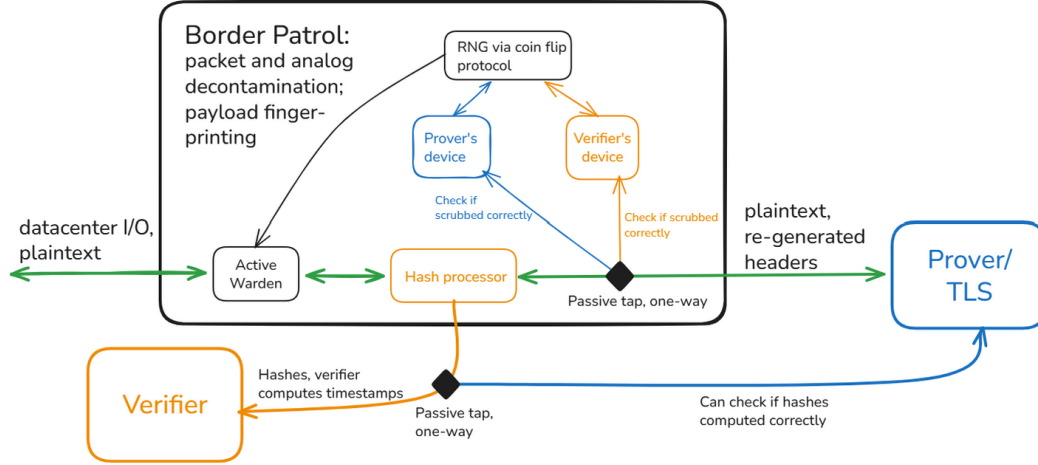


Figure 3: Caption

observe and double-check that hashes have been computed exactly as they expect, without being able to interfere with the verifier's monitor leg. Timestamps can be computed by both parties upon receiving the hashes at practically the same time. Precedents-and-Available-Hardware

3. For unfamiliar readers, TLS is the encryption between the outside world and the datacenter. Unencrypted communication within datacenters is not unusual [mbender ms, 2026]. With key escrows, or retroactive zero-knowledge proofs, or similar, we expect the proposed setup to also be adaptable for working with encrypted traffic, but here we leave this out of scope for simplicity.

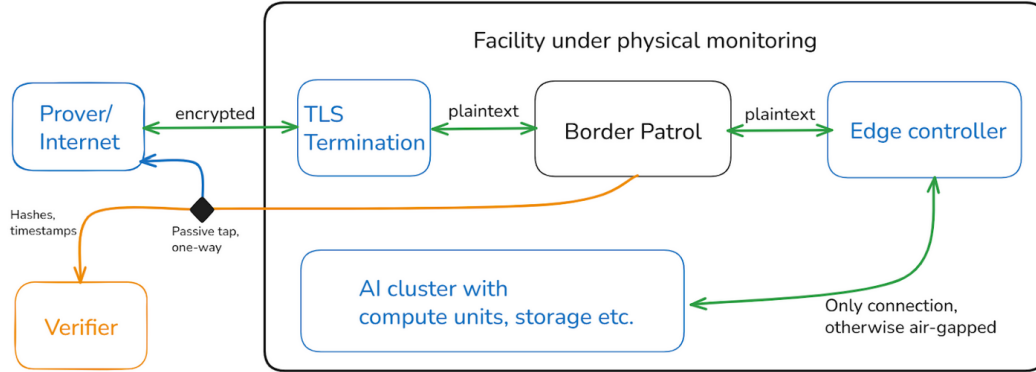


Figure 4: Caption

### The most important points about the microarchitecture (the border patrol device itself):

1. Here we also illustrate the second functionality of the border patrol device: An active warden **without supply chain trust**. While Fisk et al. [?] and Xing et al. [?] have demonstrated the elimination of steganography channels in protocol headers first in software, then in hardware, both assume single-party trust in the device. In contrast, we combine a coin flip

protocol [web, 2026b] and passive observability of the warden’s behaviour to *eliminate* the requirement of *mutual* trust in *any* device<sup>67</sup>.

2. In the illustration above, we colour-code the *minimum* device trust assumptions. This does not mean that transparent design and supply chains could not *also* establish mutual trust in components, which would further add defense in depth.<sup>8</sup>
3. Re-timing eliminates both analogue side channels (e.g. light modulation in optical fibre) as well as timing modulation at any relevant bandwidth. Re-timing is performed by the Active Warden [Uttarwar and Dakhane, 2026] device by buffering all incoming packets (e.g. for 10ms) and then sending them out in their original order at maximum bandwidth to combat attacks such as PHY-Covert Channels [?].

We present an enhanced design in the Appendix E.

## 5 Precedents and Available Hardware

While our proposal is conceptual and tested in simulation rather than real-world conditions, we emphasize that all of the individual components<sup>9</sup> for the border patrol device are either established and field-tested (passive optical fibre splitters [web], coin flip protocols [Filecoin, 2026], hash functions+timestamps [web, 2026j]<sup>10</sup>) or quickly re-configurable commercial hardware: Field-Programmable Gate Arrays (FPGAs) are a suitable choice for two reasons. Firstly, they can be adapted to any specialized application after manufacturing. [source] Secondly, they are inherently more secure against supply chain attacks, since an attacker can not anticipate the circuit design in advance. For these reasons, FPGAs find use in a range of adversarial, high-stakes environments, most notably military networks [pdf, 2026b] [web, 2025] [pdf, 2026a], high-frequency trading, financial law enforcement. FPGA network cards and network taps are commercially available from multiple vendors. [sources] [web, 2026a] These systems are deployed at scale, operate at line rate (10–400 Gb/s), introduce negligible latency, and are relied upon for regulatory compliance where evidence integrity is legally contested (e.g. Reg NMS, MiFID II [sources]). Their threat model in trading networks is explicit: traders attempt to hide behavior [source]; regulators require complete, lossless, timestamped records. A specific example is Metamako/Arista Networks, whose 7130 FPGA taps [source] are used for precision timestamping. The German stock exchange (Deutsche Börse) publicly disclosed deployment of dozens of such devices. [source]

Lastly, re-timing devices and active wardens have been built and tested at line rates exceeding 100G. scrubbing [?]/ [web, 2026k] traffic normalization [web, 2026k], and re-timing devices [Uttarwar and Dakhane, 2026] against timing and analogue side channels.

The particular combination of these components we are proposing is novel, and we simulate their behaviour using software written in Python and available on Github [derpyplods, 2026]. Our simulation works as follows:

1. A server hosts a JSON file (this is intended to replicate a datacentre hosting some output tokens stored in JSON that are intended to be sent to a user that has requested them)
2. The client requests the JSON file (this is the user that is expecting some output tokens from a language model)

---

<sup>6</sup>Why is trusted RNG required for the warden? The answer is that some network protocol headers need to include random nonces (e.g. ISNs [web, 2026i] shown at L3) for security reasons, and predictability would break this. The warden overwriting these nonces may exfiltrate information in service of the prover or verifier if not mutually observed or trusted.

<sup>7</sup>To prevent latency penalties, random nonces are not generated on-demand. Instead, the coin-flip protocol populates a pre-computed entropy buffer. The active warden consumes these numbers in a strict First-In-First-Out (FIFO) order to overwrite protocol headers at line rate.

<sup>8</sup>The information path between the verifier and the hashing processor in particular is precarious if the processor is controlled by only them. While the prover *can* observe and double-check this information, photonic or timing modulation on the outputs themselves may be dangerous channels. In appendix E, we present an extended version of the border patrol device designed to defend against such channels.

<sup>9</sup>With the possible exception of the coin flip devices. Since only unilateral trust is required, off-the-shelf CPUs, perhaps TEEs should suffice.

<sup>10</sup>Timestamps can of course be computed after the verifier and prover have received their hashes. We do not expect nanosecond-microsecond precision to be necessary here.



3. The server sends the JSON file over either TCP or UDP in a way that makes the packet stream reproducible (this is important because it is what allows the verifier to later confirm that the traffic implies no undeclared work was performed)
  - (a) Before the packets are forwarded to the client, the warden scrubs all non-reproducible components of the packets and sends them to the client
  - (b) We additionally construct the TCP and UDP packets to be deterministic, which we do by assembling the packets manually in userspace, where this would typically be done by the kernel using nondeterministic heuristics
4. We log hashes and timestamps for each packet (this simulates the passive tap)

The verifier will later run the exact same procedure on their own hardware, comparing their traffic hashes and timestamps to confirm that the prover's traffic implied they executed the same program as the verifier.

## 6 Results

For both TCP [web, 2026f] and UDP [control databases GND, 2026] traffic, we are able to detect unexpected bytes in Ethernet frames [web, 2026c]. We simulate this by having the prover send additional Ethernet frames in an attempt to send the client an additional JSON file. After scrubbing the non-reproducible fields from the frames, the comparison is trivial: the verifier compares a hash of its traffic with a hash of the prover's traffic.<sup>11</sup>

```
Test 1: UDP Reproducibility ✓ PASS

capture 1: 34 packets
capture 2: 34 packets
capture 1: 32 data frames after filtering
capture 2: 32 data frames after filtering
hash 1: 671711f2fde1e65cfb41be3078c9bd93abdc2a9cfc74a9fa7388d2b2cf84ee79
hash 2: 671711f2fde1e65cfb41be3078c9bd93abdc2a9cfc74a9fa7388d2b2cf84ee79
PASS - normalized egress traffic is identical across both runs
Result: Two identical UDP runs produce byte-for-byte identical traffic (after normalization of checksums and IP IDs).
```

Figure 5: Caption

The output of [analyze.py](#) when we run our simulation using UDP with steganography disabled. The traffic is identical, so the hashes match.

```
Test 2: UDP Tamper Detection ✓ PASS (Difference Detected)

capture 1: 34 packets
capture 2: 33 packets
capture 1: 32 data frames after filtering
capture 2: 32 data frames after filtering
hash 1: 671711f2fde1e65cfb41be3078c9bd93abdc2a9cfc74a9fa7388d2b2cf84ee79
hash 2: 78870e0e2202b0a2fab5f13ed527a27a7b734117788a7a0ff77a0e
FAIL - traffic differs
packet 0 differs
first diff at byte 92: 8a0 vs 8c08
Result: When byte 92 of the payload is 80hex (tampered), the difference is immediately detected at byte 92 (offset within the payload frame).
```

Figure 6: Caption

The output of [analyze.py](#) when we run our simulation using UDP with steganography enabled. The traffic differs, so the hashes are not equivalent.

The output of [analyze.py](#) when we run our simulation using TCP with steganography enabled. The traffic differs, so the hashes are not equivalent.

Additionally we demonstrated an attack similar to PHY-Covert Channels [?] to exfiltrate the word “SECRET” using our standard Warden device:

Our steganography simulation is drastically less sophisticated than plausible real-world steganography attempts – the prover has not made any real effort to disguise the unexpected traffic they are sending. However, it is still a demonstration of catching discrepancies in traffic using an active warden and reproducible network traffic. Further, if the traffic is entirely either reproducible or warden-generated, unless the warden is manipulated into rewriting nondeterministic fields with information the prover intends to exfiltrate *and* the verifier device’s observation of the warden’s behaviour fails, steganography

<sup>11</sup>This is somewhat different from the live-checking of the protocol headers via the verifier’s and prover’s respective devices in the border patrol machine, as shown above. The security of ISNs is not broken here since their generation seeds are kept inside the warden, but not revealed until they expire.





- We do not constrain bandwidth for covert communication *into* the datacenter. While the input data has many uncontrollable variables (media input, user prompts, ...), input wardens may re-write such information while preserving semantics. We leave this to future work.
- There still is some potential for covert outbound communication via low-frequency timing modulation, but many orders of magnitude less than without the border patrol device.

## 7.2 Future Work

- A hardware-implementation demo of our proposed setup. We expect the bill of materials of a somewhat representative device to cost less than the researcher’s and engineer’s time needed to build it.
- Threat modeling for very low outbound bandwidth—but still impactful—covert workloads in the datacenter.

## 8 Conclusion

Firstly, a brief feasibility assessment: In the appendix B, we calculate a bandwidth of ~40GB/s API egress out of a 100.000 GPU AI cluster streaming 200.000.000 tokens per second. The border patrol device, even under such extreme assumptions, can use off-the-shelf hardware. The storage requirements for both the prover and the verifier are insignificant for any realistic data management solution. Secondly, we see passive optical splitters as under-appreciated assets for designing verification setups under mutual distrust. Finally, we encourage further work on the hardware development to prepare border patrol devices for AI governance quickly, as they may be needed soon.

## Code and Data

- **Code repository:** <https://github.com/derpypl0ps/warden> [derpypl0ps, 2026]
- **Interactive demo link 1:** <https://warden-hackathon.vercel.app/> [web, 2026l]
- **Interactive demo link 2:** <https://www.felix-krueckel.com/warden.html> [web, 2026h]
- **Ethernet protocol visualization:** <https://ethernet-frame-visualization.vercel.app/> [web, 2026g]

## Author Contributions

Naci Cankaya led the project and architecture design of the border patrol machine. Jakub Kryś led the red-teaming of the security and feasibility via thought experiments and Fermi estimates. Jonathan Ng led the creation of the simulation codebase. Felix Krückel contributed the visualizations and literature research into covert communication threats. Luke Marks contributed insights into Ethernet protocol details. All authors contributed in general literature research, fact-checking and writing.

## References

- Passive optical fiber splitters. URL <https://www.keysight.com/au/en/products/network-visibility/network-taps/flex-tap-fiber-optical.html>. Accessed from keysight.com.
- Protection against supply chain attacks - sdot secure network card, 2025. URL <https://www.infodas.com/en/solutions/sdot-secure-network-card/>. Accessed from infodas.com.
- Infodas URL <https://www.criticalcommunications.airbus.com/sites/g/files/jlcbta221/files/2025-06/Infodas%20SDoT%20SecurityGateway%20Flyer.pdf>. PDF document.
- overview supply chain wp, 2026b. URL [https://ww1.microchip.com/downloads/aemdocuments/documents/fpga/ProductDocuments/SupportingCollateral/overview\\_supply\\_chain\\_wp.pdf](https://ww1.microchip.com/downloads/aemdocuments/documents/fpga/ProductDocuments/SupportingCollateral/overview_supply_chain_wp.pdf). PDF document.
- Ia-780i fpga accelerator with intel agilex 7 fpga, 2026a. URL <https://www.bittware.com/products/ia-780i/>. Accessed from bittware.com.
- Cryptographic coin flips: Commitment schemes, mpc, and verifiability, 2026b. URL <https://coinfliptool.com/articles/cryptographic-coin-flips>. Accessed from coinfliptool.com.

Ethernet frame - wikipedia, 2026c. URL [https://en.wikipedia.org/wiki/Ethernet\\_frame](https://en.wikipedia.org/wiki/Ethernet_frame). Accessed from en.wikipedia.org.

Fiber-optic splitter - wikipedia, 2026d. URL [https://en.wikipedia.org/wiki/Fiber-optic\\_splitter](https://en.wikipedia.org/wiki/Fiber-optic_splitter). Accessed from en.wikipedia.org.

Optical isolator - wikipedia, 2026e. URL [https://en.wikipedia.org/wiki/Optical\\_isolator](https://en.wikipedia.org/wiki/Optical_isolator). Accessed from en.wikipedia.org.

Transmission control protocol - wikipedia, 2026f. URL [https://en.wikipedia.org/wiki/Transmission\\_Control\\_Protocol](https://en.wikipedia.org/wiki/Transmission_Control_Protocol). Accessed from en.wikipedia.org.

Warden: Protocol stack explorer, 2026g. URL <https://ethernet-frame-visualization.vercel.app/>. Accessed from ethernet-frame-visualization.vercel.app.

Fingerprinting ai cluster usage, 2026h. URL <https://www.felix-krueckel.com/warden.html>. Accessed from felix-krueckel.com.

Warden: Protocol stack explorer, 2026i. URL <https://www.felix-krueckel.com/tcp-ip-visualizer.html>. Accessed from felix-krueckel.com.

Rfc3161 compliant time stamp authority (tsa) server, 2026j. URL <https://knowledge.digicert.com/general-information/rfc3161-compliant-time-stamp-authority-server>. Accessed from knowledge.digicert.com.

Openbsd pf: Packet filtering, 2026k. URL <https://www.openbsd.org/faq/pf/filter.html>. Accessed from openbsd.org.

Verifying agreements on compute use using trusted networking hardware, 2026l. URL <https://warden-hackathon.vercel.app/>. Accessed from warden-hackathon.vercel.app.

Onni Aarne, Tim Fist, and Caleb Withers. Secure, governable chips, 2024. URL <https://www.cnas.org/publications/reports/secure-governable-chips>. Accessed 2026-02-22.

Miles Brundage, Lennart Heim, Mauricio Baker, Gabriel Kulp, and Oliver Marks. Verifying international agreements on ai: Six layers of verification for rules on large-scale ai development and deployment, 2025. URL <https://arxiv.org/abs/2507.15916>.

Naci Cankaya. Catching misreporting about ml hardware use by turning noise into signal, 2026. URL <https://nacicankaya.substack.com/p/catching-misreporting-about-ml-hardware>. Accessed from nacicankaya.substack.com.

CeSIA and The Future Society. Global call for AI red lines, 2025. URL <https://red-lines.ai/>. Launched during the 80th session of the UN General Assembly, September 2025. Endorsed by 300+ prominent figures including 15 Nobel Prize and Turing Award recipients.

China Law Translate. Interim measures for the management of generative artificial intelligence service, 2023. URL <https://www.chinalawtranslate.com/generative-ai-interim/>. Accessed 2026-02-22.

Authority control databases GND. User datagram protocol - wikipedia, 2026. URL [https://en.wikipedia.org/wiki/User\\_Datagram\\_Protocol](https://en.wikipedia.org/wiki/User_Datagram_Protocol). Accessed from en.wikipedia.org.

derpyplods. derpyplods/warden, 2026. URL <https://github.com/derpyplods/warden>. GitHub repository.

European Parliament. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), 2024. URL <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>. Official Journal of the European Union, L 2024/1689.

Filecoin. Filecoin features: Distributed randomness & leader elections, 2026. URL <https://filecoin.io/blog/posts/filecoin-features-distributed-randomness-leader-elections>. Accessed from filecoin.io.

Gina Fisk, Mike Fisk, Christos Papadopoulos, and Joshua Neil. Eliminating steganography in internet traffic with active wardens. In Fabien A. P. Petitcolas, editor, *Information Hiding*, pages 18–35, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg. ISBN 978-3-540-36415-3.

- FlexHEG Initiative. Flexible hardware-enabled guarantees for ai compute, 2025. URL <https://flexheg.com/>. A joint initiative by Convergent Research and Advanced Research and Invention Agency.
- Jonathan Happel. Tampersec, 2026. URL <https://tampersec.com/>.
- Ben Harack, Robert F. Trager, Anka Reuel, David Manheim, Miles Brundage, Onni Aarne, Aaron Scher, Yanliang Pan, Jenny Xiao, Kristy Loke, Sumaya Nur Adan, Guillem Bas, Nicholas A. Caputo, Julia C. Morse, Janvi Ahuja, Isabella Duan, Janet Egan, Ben Bucknall, Brianna Rosen, Renan Araujo, Vincent Boulanin, Ranjit Lall, Fazl Barez, Sanaa Alvira, Corin Katzke, Ahmad Atamli, , and Amro Awad. Verification for international ai governance, 2025. URL <https://aigi.ox.ac.uk/publications/verification-for-international-ai-governance/>. Accessed 2026-02-22.
- Adam Karvonen, Daniel Reuter, Roy Rinberg, Luke Marks, Adrià Garriga-Alonso, and Keri Warr. Difr: Inference verification despite nondeterminism, 2025. URL <https://arxiv.org/abs/2511.20621>.
- Ki Suh Lee, Han Wang, and Hakim Weatherspoon. PHY covert channels: Can you see the idles? In *11th USENIX Symposium on Networked Systems Design and Implementation (NSDI 14)*, pages 173–185, Seattle, WA, April 2014. USENIX Association. ISBN 978-1-931971-09-6. URL <https://www.usenix.org/conference/nsdi14/technical-sessions/presentation/lee>.
- mbender ms. Enabling end to end tls on azure application gateway, 2026. URL <https://learn.microsoft.com/en-us/azure/application-gateway/ssl-overview>. Accessed from learn.microsoft.com.
- OpenAI. Chat Completions streaming events. <https://developers.openai.com/api/reference/resources/chat/subresources/completions/streaming-events>, 2025. OpenAI API Reference. Accessed: 2026-02-25.
- James Petrie. Guaranteeable memory: An HBM-based chiplet for verifiable AI workloads. In *ICML Workshop on Technical AI Governance (TAIG)*, 2025. URL <https://openreview.net/forum?id=uc79kOv0MV>.
- Roy Rinberg, Adam Karvonen, Alexander Hoover, Daniel Reuter, and Keri Warr. Verifying llm inference to detect model weight exfiltration, 2025. URL <https://arxiv.org/abs/2511.02620>.
- Girish Sastry, Lennart Heim, Haydn Belfield, Markus Anderljung, Miles Brundage, Julian Hazell, Cullen O’Keefe, Gillian K. Hadfield, Richard Ngo, Konstantin Pilz, George Gor, Emma Bluemke, Sarah Shoker, Janet Egan, Robert F. Trager, Shahar Avin, Adrian Weller, Yoshua Bengio, and Diane Coyle. Computing power and the governance of artificial intelligence, 2024. URL <https://arxiv.org/abs/2402.08797>.
- Aaron Scher and Lisa Thiergart. Mechanisms to verify international agreements about ai development, 2024. URL <https://techgov.intelligence.org/research/mechanisms-to-verify-international-agreements-about-ai-development>. Accessed 2026-02-22.
- Vrushali Uttarwar and Dhananjay Dakhane. Delay normalization technique to disrupt covert timing channels using active warden. *EPJ Web of Conferences*, 328, 06 2025. doi: 10.1051/epjconf/202532801049.
- Vrushali Uday Uttarwar and Dhananjay M. Dakhane. Delay normalization technique to disrupt covert timing channels using active warden | epj web of conferences, 2026. URL [https://www.epj-conferences.org/articles/epjconf/abs/2025/13/epjconf\\_icetsf2025\\_01049/epjconf\\_icetsf2025\\_01049.html](https://www.epj-conferences.org/articles/epjconf/abs/2025/13/epjconf_icetsf2025_01049/epjconf_icetsf2025_01049.html). Accessed from epj-conferences.org.
- Scott Wiener. SB-53: Artificial intelligence models: Large developers, 2025. URL [https://leginfo.ca.gov/faces/billNavClient.xhtml?bill\\_id=202520260SB53](https://leginfo.ca.gov/faces/billNavClient.xhtml?bill_id=202520260SB53). California Senate Bill 53, Chapter 138, Statutes of 2025. Approved by Governor September 29, 2025.
- Jiarong Xing, Qiao Kang, and Ang Chen. NetWarden: Mitigating network covert channels while preserving performance. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 2039–2056. USENIX Association, August 2020. ISBN 978-1-939133-17-5. URL <https://www.usenix.org/conference/usenixsecurity20/presentation/xing>.
- Steven Clare Yoshua Bengio, C. Prunkl, M. Murray, M. Andriushchenko, B. Bucknall, R. Bommasani, S. Casper, T. Davidson, R. Douglas, D. Duvenaud, P. Fox, U. Gohar, R. Hadshar, A. Ho, T. Hu, C. Jones, S. Kapoor, A. Kasirzadeh, S. Manning, N. Maslej, V. Mavroudis, C. McGlynn, R. Moulange, J. Newman, K. Y. Ng, P. Paskov, S. Rismani, G. Sastry, E. Seger, S. Singer, C. Stix,

L. Velasco, N. Wheeler, D. Acemoglu, V. Conitzer, T. G. Dietterich, E. W. Felten, F. Heintz, G. Hinton, N. Jennings, S. Leavy, T. Ludermir, V. Marda, H. Margetts, J. McDermid, J. Munga, A. Narayanan, A. Nelson, C. Neppel, S. D. Ramchurn, S. Russell, M. Schaaake, B. Schölkopf, A. Soto, L. Tiedrich, G. Varoquaux, A. Yao, Y.-Q. Zhang, L. A. Aguirre, O. Ajala, F. Albalawi, N. AlMalek, C. Busch, J. Collas, A. C. P. de L. F. de Carvalho, A. Gill, A. H. Hatip, J. Heikkilä, C. Johnson, G. Jolly, Z. Katzir, M. N. Kerema, H. Kitano, A. Krüger, K. M. Lee, J. R. López Portillo, A. McLysaght, O. Molchanovskiy, A. Monti, M. Nemer, N. Oliver, R. Pezoa, A. Plonk, B. Ravindran, H. Riza, C. Rugege, H. Sheikh, D. Wong, Y. Zeng, L. Zhu, D. Privitera, and S. Mindermann. International ai safety report 2026, 2026. URL <https://internationalaisafetyreport.org>.

## Appendices

### A Prover’s Verification Mechanism

We now consider the problem of how verification of such hashed values could take place. The fundamental challenge is as follows: given a hash value chosen by the Verifier out of the annual pool of hashes, how can the Prover reliably and efficiently demonstrate that they possess a record entry which hashes to this value<sup>12</sup>?

A simple idea is to maintain a traditional ‘hash table’ – a dictionary of all plaintext LLM inputs, the corresponding plaintext outputs and their hash values. Since the Prover already controls the egress from the data centre, they can easily register how many Ethernet frames each output gets broken into. Furthermore, since the Border Patrol protocol would be fully open-source, they also know the ‘hashing boundary’ – how many frames are included in one hash. This allows the Prover to have a causal association between a prompt, the plaintext output and the corresponding sequence of hashes. The hash values flow back to the Prover through a passive network tap placed on the connection which carries them from the Border Patrol to the verification cluster (see Fig. 2).

This in turn can be used for an extremely efficient hash lookup. When the Verifier specifies the hash whose provenance is to be demonstrated, the Prover finds the key associated with this hash and forwards it to the secure verification facility for replay. The facility recomputes the hash and presents it to the Verifier, who is then satisfied that the Prover must have carried out a workload that produces this hash.

The Border Patrol protocol needs to agree on the number of Ethernet frames corresponding to the fundamental ‘verification unit’ that gets hashed. This number is arbitrary and should strike a balance between storage requirements and recomputation time. At the extreme end of the spectrum, we could hash every single Ethernet frame, leading to the highest possible number of hashes in storage. However, since in this scenario one hash corresponds to a very small number of output tokens, this minimises the number of outputs that need to be recomputed in the verification facility. On the other hand, we could hash together all Ethernet frames that pass the Border Patrol within a month, which would lead to only one hash in storage, but would require one month of recomputation during verification.

The Prover needs to maintain knowledge of which inputs and parts of the corresponding outputs were included in each hash. For example, assume that the hashing window is 150 Ethernet frames, two input prompts generate 120 and 70 tokens, respectively, and one output token is streamed out via a single Ethernet frame. The Prover must then associate the following with the hash values h1 and h2:

```
““
{
h1: [(prompt_1, output_1, 1, 120), (prompt_2, output_2, 1, 30)],
h2: [(prompt_2, output_2, 31, 70), ...],
...
} ““
```

<sup>12</sup>Once again, in this work we do not consider the problem of verifying that this declared workload is compliant with some regulations, only the problem of verifying that no other undeclared workloads have been run.

In this way, when the Verifier demands that hash h1 be reproduced, the Prover can immediately look up the fact that prompts 1 and 2 must be sent out to the verification facility<sup>13</sup> (alongside the corresponding outputs and their indices). This information is necessary for the verification facility to faithfully reproduce the exact stream of 150 Ethernet frames that should be hashed and compared to h1.

## B Storage Requirements

We start by calculating an upper estimate of the volume of the hashes and plaintext data that would be required to be stored by the verifier and prover respectively. We assume worst-case conditions in order to demonstrate the feasibility of our proposal.

First, let us assume that the datacenter under monitoring contains 100k GPUs of the NVIDIA Hopper generation. Each such GPU is assumed to be capable of a 2000 token/s inference throughput<sup>14</sup>, meaning that the total throughput of the cluster is  $2 \cdot 10^8$  tokens/s. Next, we need to calculate how many bytes of data this token volume corresponds to. For this, we assume that the tokens are wrapped in OpenAI’s streaming API template of the following format:

```
““ {“id”:“chatcmpl-123”,“object”:“chat.completion.chunk”,“created”:1694268190,“model”:“gpt-4o-mini”,“system_fingerprint”:“fp_44709d6fcb”,“choices”: [{“index”:0,“delta”: {“content”:“Hello”},“logprobs”:null,“finish_reason”
```

Importantly, note that this template includes a single response token only. This is because the streaming API aims to deliver generated tokens to the user as quickly as possible, rather than waiting for the full generation to finish before sending the payload. The ‘one-token-per-json’ scenario represents the most challenging configuration for our methodology, as this will lead to the highest possible number of hash computations.

Furthermore, we operate under an (unrealistic) assumption that each such template is allocated to one Ethernet frame. The payload is around 200 ASCII characters (see the streaming format above), corresponding to 200 bytes (+ headers) – well below the Maximum Transmission Unit (MTU) of the Ethernet protocol.

Therefore, the total number of Ethernet frames streamed out of the cluster is simply  $2 \cdot 10^8$  per second, same as tokens. We then calculate the SHA-256 hash of each such frame, leading to  $2 \cdot 10^8 \cdot 24 \cdot 3600 \cdot 365 = 6.3 \cdot 10^{15}$  hash computations performed in a year, with a corresponding hash volume of  $6.3 \cdot 10^{15} \cdot 256 / 8 = 2 \cdot 10^{17}$  bytes  $\sim 200$ PB.

Additionally, the Prover needs to maintain a year-long record of all plaintext data transmitted from their cluster to the outside world. Each token generated in their cluster is assumed to be wrapped in the template above. Since one ASCII character is stored by exactly 1 byte, this means that to stream one token out of the cluster, 200 bytes are required. On an annual scale, this corresponds to  $2 \cdot 10^8 \cdot 200 \cdot 24 \cdot 3600 \cdot 365 = 1.26 \cdot 10^{18}$  bytes  $\sim 1,260$ PB.

The cost of storing such a large amount of data is small compared to the costs of AI datacenters at the scale considered here (<1%): A typical price for a 28TB HDD hard drive is around 500€<sup>15</sup>, thus the full cost amounts to  $1,260 \text{ PB} / 28 \text{ TB} \cdot 500 \text{ €} \sim 20,000,000 \text{ €}$ .

Note that all these estimates represent a pessimistic upper bound that arises from *extremely* inefficient data management. When using non-streaming APIs, multiple tokens are included as part of one chat completion template. Further, multiple such templates could be transmitted as part of a single Ethernet frame, as long as the total payload size does not exceed the standard Ethernet MTU of 1500 bytes. Storing API json files for each token is also likely unnecessary when they can be reconstructed from tokens and heuristics. We did not include data compression at all.

Finally, we do not need to compute the hash of each Ethernet frame. Instead, the ‘fundamental unit’ of verification could be an arbitrarily long chain of frames. All these modifications would reduce storage by >3 orders of magnitude.

<sup>13</sup>Note that in general, these could be batched prompts or some other type of input. We used single prompts for simplicity in this illustrative example.

<sup>14</sup>Deepseek’s inference setup for their v3/R1 models is reported to achieve a token throughput of [~14.8k tokens per H800 node](#) (8 GPUs, decode unit) per second.

<sup>15</sup>As of early 2026



## C Preventing dictionary attacks

The Prover might be worried that the Verifier can deduce the plaintext content of the messages passing through the Border Patrol by guessing which content hashes to the observed hash values. Calculating this content by inverting the hash is not possible – hash functions are by design irreversible. However, an adversarial Verifier could be tempted to use so-called dictionary attacks. In other words, they could pre-compute the hashes of the most common plausible inputs and simply compare them to the observed ones. The feasibility of this approach is entirely determined on the expected size of the input space of the hash function. For example, if there can only ever be 10 possible inputs, then it is trivial to pre-compute their 10 corresponding hashes and infer the input that has produced the hash coming out of the Border Patrol.

Unfortunately for the Prover, the input space of their API responses is indeed somewhat limited: these can only be tokens generated by the LLM<sup>16</sup>. These in turn are constrained by the size of the LLM vocabulary, typically around 200 000 tokens. Thus, in the scenario presented above – where only one output token is inserted into the streaming completion template, this template corresponds to one Ethernet frame and later one hash – the attacker could pre-compute the hashes of all tokens inserted into these templates. They would then simply perform the lookup in a hash table with 200 000 values and immediately infer the right token. Thus, it would be trivial for the Verifier to guess all the tokens from the streaming API responses.

To calculate how many tokens need to be inserted into the chat template to prevent such attacks through combinatorial complexity, let us consider how many hash computations a motivated attacker could perform in a month. Specialised chips can achieve throughputs of 200TH/s (terahashes per second). Within a month, this corresponds to  $5.2 \cdot 10^{20}$  hashes computed. On the other hand, a sequence of  $n$  output tokens out of a 200k vocabulary can lead to  $(2 \cdot 10^5)^n$  distinct inputs. Thus, the attacker is guaranteed to guess the sequence corresponding to a given hash if the sequence is shorter than  $\log_{2 \cdot 10^5}(5.2 \cdot 10^{20}) \sim 3.9$  tokens long. Running multiple specialised chips in parallel will not help the attacker much – with 1000 hash-crunching chips, the token number increases to 4.5.

Overall, to be on the safe side, the streaming API template should enclose at least 5 tokens in order to prevent brute-force hash guessing by the Verifier. However, this back-of-the-envelope calculation assumes that the attacker needs to try all possible  $n$ -gram combinations of tokens from the vocabulary. This is a totally unrealistic assumption, as the tokens streamed out of the cluster will almost always be semantically meaningful – sequences of tokens that form sentences, code snippets, equations, or similar. Thus, the search space is massively reduced by noting that only a small fraction of the vocabulary is likely to follow a token like ‘The’. Assuming that only 1000 most likely tokens need to be checked, our ‘effective vocabulary’ is reduced to 1000. Then, the calculation becomes  $\log_{2 \cdot 10^5}(5.2 \cdot 10^{20}) \sim 7$ . In other words, any semantically meaningful sequence of fewer than 7 tokens could be brute-forced by the Verifier in less than a month with a single hash-crunching chip. Thus, to prevent this, the streaming API output template could wrap at least 10 tokens. This should have a negligible effect on user experience – instead of seeing tokens appear on their screen one at a time, the user will receive them 10 at a time. Alternatively (or additionally), the hashes could simply be computed on more than one JSON template or more than one Ethernet frame. For example, if the hashing boundary is set every 100 Ethernet frames, the whole problem disappears even with 1 streaming token per JSON template.

## D Eliminating steganography needs connection tables

The need to prevent steganographic communication between the data centre and the outside world introduces the need to eliminate certain degrees of freedom from the protocol metadata. To illustrate

<sup>16</sup>The surrounding chat completion template that encompasses the output tokens is also a part of the content that gets hashed. However, there are no degrees of freedom there. To understand why, first note that the verification cluster replays the workload using the provided inputs, inserts the output tokens into the completion template, hashes this JSON object and compares it to the observed hash from the Border Patrol. However, the replayed computation will have a different timestamp and fingerprint to the one that produced the original hash. Thus, the Prover needs to supply the verification cluster not only with the input prompt, but also the exact metadata in the output template. In other words, the Prover declares: ‘Here is the right prompt and the corresponding template metadata, but not the output itself’. Thus, the only degree of freedom is really limited to the output tokens.



this more concretely with an example, in this Appendix we justify why source and destination ports need to be explicitly handled by the Active Warden.

Network protocols grant both communication parties control over certain protocol fields. In UDP, the initiating party (client) selects its source port, whilst the responding party (server) must use the destination port specified in the request as its source port for the response. Without intervention, either party could encode information through port selection.

Consider a simple example: an external client initiating API requests to a datacenter. By choosing source port 5000 versus 5001, the client transmits one bit of information per connection. At 1000 requests per second, this yields 125 Bps or  $\sim 10$  GB/day of covert channel capacity. Similarly, when the datacenter initiates outbound connections (e.g., fetching training data), it could encode information in its choice of ephemeral source port (typically ranging from 32768 to 60999, providing  $\sim 15$  bits per connection). The Active Warden must eliminate both channels.

Two separate connection tracking tables are required, because connections can be initiated from either direction:

- **External-initiated connections** (e.g. API requests to the datacenter) allow an external client to encode information in their choice of client source port. The warden must replace this with a random value, then maintain state to translate responses back to the original port.
- **Datacenter-initiated connections** (e.g. fetching external datasets) allow the datacenter operator to encode information in their choice of client source port. Again, the warden must replace this with a joint random value and maintain a reverse translation state.

These cannot share a single table because the same port number (for example, 5001) might be simultaneously assigned to a datacenter client port in one connection and to an external client port in another. The tables must be keyed by the full connection 4-tuple: (source IP, source port, destination IP, destination port) in order to disambiguate these two potentially conflicting cases.

Each state-tracking table has two distinct security functions during the connection lifecycle. First, during the request phase, the table performs port randomisation: the initiating party's source port (client port) is replaced with a value from the RNG, eliminating their ability to encode information. Simultaneously, the table records the target server port from the request's destination field. During the response phase, the table performs enforcement and back-translation: it verifies the responding party uses the correct server source port (which prevents the server from encoding information through port choice), and it translates the response destination port from the RNG value back to the original client port. This ensures that the response is delivered to the correct client port and does not carry covert information through the choice of the server port.

Similar translation tables need to be maintained wherever parts of the relevant network protocol offer the attacker degrees of freedom that could be used for steganographic communication. This could introduce significant programmatic complexity for more complicated protocols like TCP, which are stateful. In TCP, the Active Warden must additionally perform sequence number translation on every single packet, and in both directions. More precisely, during the so-called 'TCP handshake' the client's Initial Sequence Number (ISN) is replaced with a random number. Thus, the Warden must record the offset between the original and scrubbed ISN, so that all subsequent packets in this connection have their outbound sequence numbers incremented by this offset. Similarly, the corresponding inbound ACK numbers in this connection need to be decremented by the same offset. This is necessary to maintain consistency in both the original and scrubbed sequences. Overall, the Active Warden must track connection state to handle the handshake phase, data transfer phase, and connection termination. Each TCP connection might require around 200 bytes of state-tracking data. For a data centre with  $O(1000)$  concurrent connections processing millions of packets per second, the Active Warden must implement efficient hash lookups to avoid slowdowns in serving this traffic to customers.

## E Enhanced design for the border patrol device

The architecture shown below combats timing and analog modulation side-channels between the verifier and their hash processor in the border patrol device. We refer to Uttarwar et al. [Uttarwar and Dakhane, 2026] for more details on the timing warden. Another enhancement here is passive observation on both sides of the active warden.

Test 5: TCP Steganography Detection ✓ PASS (Difference Detected)

```
capture 1: 40 packets
capture 2: 39 packets
capture 1: 35 data frames after filtering
capture 2: 34 data frames after filtering
hash 1: f64b012dbba0be07871a88b005892b6a8964ba88beeb808e798adde3589856b
hash 2: 1f33882b1c082d8a4ac2781600520a4bf35bba1b8d06f63126f8e957eacce
FAIL - traffic differs
packet 10 differs
  first diff at byte 14: 0x45 vs 0x47
  context 1: 0000010800450005dc000040004006
  context 2: 0000010800470005dc000040004006
[packets 11-15 also show byte 14 differences: 0x45 vs 0x47]
packet 16-34 show TCP sequence number differences due to payload size variations
```

**Result:** The steganographic TCP scenario (with hidden message in IP options) is successfully detected:

- **Detection point:** Packets 10-15 show the key difference at byte 14
- **What changed:** The IP header length (IHL) field from 0x45 to 0x47
  - 0x45 = Version 4, IHL 5 (20 bytes) - normal TCP
  - 0x47 = Version 4, IHL 7 (28 bytes) - TCP with 8-byte IP options
- **Why it matters:** The 8-byte IP options contain the hidden steganographic message
- **Covert channel exposed:** The presence of the "SECRET" message hidden in IP padding is revealed through the IHL field change

The implementation successfully demonstrates that **IP padding-based steganography is detectable through traffic analysis** - the analyze.py tool caught the covert channel by comparing normalized traffic patterns and identifying structural differences in the IP headers.